

**UNITED STATES DISTRICT COURT  
DISTRICT OF MINNESOTA**

---

Civil File No.: 22-cv-00254-WMW-DTS

ImageTrend, Inc.,

Plaintiff,

vs.

**VERIFIED AMENDED COMPLAINT**

Locality Media, Inc. d/b/a First Due,  
Richard Dutcher, Richard French, Anne  
Hulsether, Victoria Koistinen, and Nicholas  
Spring,

Defendants.

---

For its Verified Amended Complaint against Defendants Locality Media, Inc. d/b/a/ First Due, Richard Dutcher, Richard “Chris” French, Anne Hulsether, Victoria Koistinen, and Nicholas Spring, Plaintiff ImageTrend, Inc. states and alleges as follows:

**INTRODUCTION**

1. Plaintiff ImageTrend, Inc. (“ImageTrend”) is a leading software solutions company that provides an established suite of connected solutions for fire and emergency medical services (“EMS”) departments, including an EMS electronic patient care record system, staff scheduling software, fire rescue management systems, reporting and analytics, inventory, checklists, training and activities management solutions (collectively, “Elite Platform”). The Elite Platform is a “cloud solution” – ImageTrend’s customers connect to Elite via the internet. Elite is used in and intended for use in interstate commerce.

2. Defendant Locality Media, Inc. d/b/a First Due (“First Due”) is a new competitor software company offering a limited pre-plan solution to fire departments. Prior to 2021, First Due did not offer any comparable or competitive EMS products or software solutions to ImageTrend’s Elite product. Presently, First Due is marketing and selling a fire rescue management platform and is advertising the development of a competitive EMS platform.

3. Approximately one year ago, First Due commenced a targeted and focused scheme to poach employees from its competitors, including ImageTrend. First Due has a pervasive plan to target and solicit ImageTrend employees in order to advance its desire to develop a competitive connected EMS and fire software platform. As part of this scheme, First Due encouraged ImageTrend employees to misappropriate ImageTrend’s intellectual property before leaving ImageTrend and joining First Due. First Due’s actions have resulted in misappropriation and destruction of intellectual property, tortious interference with ImageTrend’s current and prospective contractual relations, and conversion of confidential and proprietary information.

4. First Due’s unlawful conduct has continued to escalate and become more brazen over time. Recently, ImageTrend discovered that First Due solicited and encouraged First Due employees, former ImageTrend employees, and a current ImageTrend client to surreptitiously access ImageTrend’s confidential and proprietary production sites in order to steal confidential intellectual property and reverse-engineer ImageTrend’s intellectual property. This unauthorized access not only exposed ImageTrend’s proprietary and confidential information, but it also compromised

confidential client data and protected patient health information in violation of various state and federal laws, resulting in extraordinary damages. First Due's unlawful conduct continues.

5. As a result of First Due's unlawful conduct, ImageTrend has suffered immense damages including the misappropriation and destruction of its intellectual property, tortious interference with ImageTrend's current and prospective contractual relations, and conversion of confidential and proprietary information.

### **PARTIES**

6. Plaintiff ImageTrend is a Minnesota corporation with its corporate headquarters located at 20855 Kensington Boulevard in Lakeville, Minnesota.

7. Defendant First Due is a Delaware corporation with its corporate headquarters located at 107 7th Street in Garden City, New York. First Due regularly conducts business in Minnesota.

8. Defendant Richard Dutcher ("Dutcher") is a Minnesota resident residing at 25726 Quagga Street Northwest in Zimmerman, Minnesota. Dutcher is a former employee of ImageTrend and is currently employed by First Due.

9. Upon information and belief, Defendant Richard "Chris" French ("French") is an individual residing in Virginia. French is an employee both of First Due and the Staunton, Virginia Fire Department.

10. Defendant Anne Hulsether ("Hulsether") is a Minnesota resident residing at 16862 Interlachen Boulevard in Lakeville, Minnesota. Hulsether is a former employee of ImageTrend and is currently employed by First Due.

11. Defendant Victoria Koistinen (“Koistinen”) is a Minnesota resident residing at 956 Randolph Avenue in St. Paul, Minnesota. Koistinen is a former employee of ImageTrend and is currently employed by First Due.

12. Defendant Nicholas Spring (“Spring”) is a Minnesota resident residing at 1031 Meadow Street in Cologne, Minnesota. Spring is a former employee of ImageTrend and is currently employed by First Due.<sup>1</sup>

### **JURISDICTION AND VENUE**

13. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 and 28 U.S.C. 1367(a).

14. This Court has personal jurisdiction over First Due because First Due has availed itself to the jurisdiction of this Court through sufficient minimum contacts, including regularly conducting business in Minnesota at all times relevant hereto.

15. This Court has personal jurisdiction over Dutcher, Hulsether, Koistinen, and Spring because they are Minnesota residents.

16. This Court has personal jurisdiction over French because his acts of misconduct occurred in Minnesota in that they were perpetrated upon information technology resources and assets that are physically located in Minnesota and caused damage to ImageTrend in Minnesota. This Court also has personal jurisdiction over French because he participated in a tortious conspiracy by accessing ImageTrend’s information

---

<sup>1</sup> Defendants Dutcher, Hulsether, Koistinen, and Spring are collectively referred to herein as the “Departed Employees.”

technology resources that are physically located in Minnesota, the effect of which is felt in Minnesota.

17. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to the claims asserted herein occurred or had effects in this District and because all of the Defendants have lived and/or conducted business and/or the acts of misconduct occurred in this jurisdiction.

### **BACKGROUND**

#### **The Importance of ImageTrend Protecting Intellectual Property and Trade Secrets**

18. ImageTrend is a leading software solutions company providing a comprehensive and connected suite of solutions for data collection, incident response and resource management, reporting, and analytics, for public safety organizations across the country.

19. The public safety software solutions industry is highly competitive, with success predicated on the development of cutting-edge technology and forward-thinking innovations. ImageTrend has been able to succeed within this highly competitive industry over the course of the past 24 years through constant innovation and a relentless commitment to providing superior products and client services.

20. Protecting its intellectual property and maintaining the confidentiality of its trade secrets are of vital importance to ImageTrend. ImageTrend has developed and maintained strict administrative, physical, and technical safeguards throughout its infrastructure and supporting processes to protect against any reasonably anticipated

threats or hazards to the security or integrity of confidential information, including, but not limited to, implementation of multifactor authentication, database and laptop encryption, strict firewall controls at authorization boundaries, intrusion detection and prevention technologies, meticulous audit and system access reporting, acceptable use policies, client contracts, and required annual HIPAA compliance and security training for all ImageTrend employees.

21. In addition, and to this end, all of ImageTrend's employees are governed by and subject to the ImageTrend Intellectual Property Policy ("IP Policy"). The IP Policy notifies ImageTrend employees that it "is vital to maintain the confidentiality of ImageTrend Assets for competitive, security and other business reasons, as well as to comply with securities and other laws."

22. As a result, the IP Policy provides that all of ImageTrend's employees "shall [1] "[r]efrain from disclosing any Proprietary and/or Confidential Information to third parties, except as expressly provided"; [2] "[t]ake reasonable security precautions to keep confidential the Proprietary and Confidential Information"; [3] "[r]efrain from disclosing, reproducing, summarizing and/or distributing Proprietary and Confidential Information except as permitted in the regular course of business"; [and 4] "[r]efrain from reverse engineering, decompiling or disassembling any software code except as permitted in the regular course of business."

23. ImageTrend's Acceptable Use Policy provides, [1] "ImageTrend proprietary information stored on electronic and computing devices whether owned or leased by ImageTrend, the employee or a third party, remains the sole property of ImageTrend"; and

[2] “ImageTrend proprietary information includes ImageTrend intellectual property like UI design, database schema, manuals or other document deliverables, roadmaps, customer lists, sales opportunities, templates, pricing information, trade secrets, or any other information which could cause damage to ImageTrend if inappropriately disclosed, or any information which a competitor could use to gain inappropriate advantages against ImageTrend.” Furthermore, ImageTrend’s Acceptable Use Policy strictly prohibits: [1] “Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations,” [2] “Accessing data, a server or an account for any purpose other than conducting ImageTrend business, even if you have authorized access,” [3] “Revealing your account password to others or allowing use of your account by others,” [4] “Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties,” and [5] “Providing information about, or lists of, ImageTrend employees to parties outside ImageTrend.”

24. The IP Policy further provides: “In addition to the obligation of nondisclosure, employees are required to use Proprietary and/or Confidential Information only in connection with our business. These obligations apply whether or not employees develop the information themselves.” Noncompliance with ImageTrend’s Acceptable Use Policy may result in disciplinary action up to and including termination of employment.

25. The Departed Employees each signed the ImageTrend Intellectual Property Agreement. All ImageTrend employees are subject to the ImageTrend Acceptable Use Policy.

### **First Due Begins Poaching ImageTrend Employees**

26. First Due entered the public safety market as a niche player offering a limited pre-plan solution to fire departments. Prior to 2021, First Due did not offer any comparable or competitive EMS products or software solutions to ImageTrend's Elite product.

27. On January 11, 2021, Justin Dillard and Joseph Robinson abruptly resigned from their employment with ImageTrend. Dillard, an Elite Product Sales Executive, and Robinson, an Account Executive, both informed ImageTrend that they were leaving to work for First Due.

28. On or about July 12, 2021, an ImageTrend employee was contacted by Dillard, who sought to recruit that employee to join First Due. Dillard disclosed that it was First Due's plan to recruit ImageTrend employees *en masse*. Dillard went so far as to represent that First Due's Chief Executive Officer had granted him authority to hire ImageTrend employees without interviews.

29. In the months that followed, First Due executed its plan to recruit as many ImageTrend employees as possible. Worse, First Due induced several of the ImageTrend employees it recruited to steal ImageTrend's intellectual property—both during and after their departures—in violation of the contractual, common law, and statutory duties they owed to ImageTrend.



30. On August 2, 2021, Toby Ritt, then ImageTrend's Vice President of Sales, and Hulsether, then ImageTrend's Director of Sales and former Director of Client Services, both resigned. Like Dillard and Robinson, Ritt and Hulsether informed ImageTrend that they were leaving for First Due. Both Ritt and Hulsether were recruited by Dillard and Robinson.

**ImageTrend Discovers Theft by Employees Departing for First Due**

31. After Ritt and Hulsether departed, ImageTrend began a review of electronically stored information accessed or created by Ritt and Hulsether prior to their resignations. As a member of ImageTrend's Executive Leadership Team ("ELT") and Vice President of Sales, Ritt had access to or created highly sensitive confidential information, including, but not limited to ELT meeting notes, ImageTrend strategic business plans, financial and investment information, employee compensation, retention and recruiting strategies, sales and customer information, and intimate knowledge regarding ELT's discussion surrounding First Due's solicitation scheme.

32. Hulsether, in her roles as ImageTrend's Director of Sales and Director of Client Services, had access to or created highly sensitive confidential information, including, but not limited to, prospective sales leads reports, client contact information, client support cases, client implementation plans, client contracts, custom development planning, and intimate knowledge regarding ImageTrend's comparative market and product analysis of First Due.

33. Upon information and belief, Ritt and Hulsether were hired by First Due to solicit ImageTrend's current and prospective clients and poach ImageTrend employees.

34. ImageTrend's employee community, customer base, and prospective client leads were developed over significant time and at substantial expense to ImageTrend.

35. Upon further information and belief, First Due induced Ritt and Hulsether to steal the aforementioned highly sensitive confidential information as part of its recruitment of Ritt and Hulsether.

36. Upon information and belief, Hulsether interviewed with First Due in July 2021. First Due offered Hulsether a job (which Hulsether accepted). According to First Due's offer letter, which was discovered on Hulsether's ImageTrend computer, Hulsether's start date as a First Due employee was July 27, 2021. Hulsether, however, did not resign from her employment with ImageTrend until August 2, 2021. Unbeknownst to ImageTrend, Hulsether was therefore an employee of First Due while she was still an employee of ImageTrend for approximately one week.

37. Upon information and belief, during the interview process with First Due, Hulsether used and distributed ImageTrend documents containing confidential and proprietary system processes and procedures, client information, and client-specific project implementation data to First Due.

38. On July 23, 2021 (after Hulsether had accepted a position with First Due but was still employed with ImageTrend), Hulsether connected a separate computer hard drive to her ImageTrend computer. While the USB device was installed, Hulsether accessed confidential and proprietary ImageTrend information, including information on ImageTrend's shared network drive. Among the information accessed and, upon information and belief, stolen by Hulsether was a document entitled

“Marketing\_Full\_Customer\_List\_All\_23-Jul-2021\_14-31.xlsx”. This document contained a comprehensive list of ImageTrend’s current customers and their contact information. The separate computer hard drive has not been returned to ImageTrend.

39. Also on July 23, 2021, Hulsether attached two documents to an email from her personal Gmail account: A PowerPoint presentation named “CSELT” and an Excel spreadsheet named “200\_100Project Charter\_2021”. The CSELT PowerPoint contained strategic planning information known and distributed only to ImageTrend executive leadership. The “200\_100Project Charter\_2021” spreadsheet contained specific information regarding a current project implementation plan for ImageTrend’s largest client.

40. Hulsether also accessed both Spring and Koistinen’s resumes on July 22 and July 23 respectively – while she was still an employee of ImageTrend. Upon information and belief, Hulsether was already soliciting Spring and Koistinen to leave ImageTrend to become First Due employees while she was still employed by ImageTrend.

41. On July 19, July 20, July 21, July 28 and August 2, 2021 (the day Hulsether resigned from ImageTrend but was also employed by First Due), Hulsether connected a flash drive to her ImageTrend computer. Upon information and belief, Hulsether misappropriated additional ImageTrend information on to this flash drive. This flash drive has not been returned to ImageTrend.

42. The day after her resignation, Hulsether contacted and solicited numerous ImageTrend clients on behalf of First Due. During these solicitations, Hulsether disclosed

ImageTrend's highly confidential and proprietary information, including current and future business plans and strategies known only within ImageTrend's senior management.

43. On August 4, 2021, ImageTrend raised its concerns regarding First Due's unlawful solicitation of its employees directly with a member of First Due's board of directors.

44. On August 26, 2021, First Due's CEO, Andreas Huber, emailed ImageTrend's President directly to address ImageTrend's concerns that First Due was unlawfully soliciting its employees. In that communication, First Due expressly represented that: (1) First Due does not "directly recruit employees from specific companies" and that it was not "targeting" ImageTrend employees; (2) all employment agreements were reviewed to ensure First Due was not "violating any laws or agreements" in its recruiting; (3) First Due employees are required to sign agreements that "mandate[] they do not bring or utilize any confidential information, IP, or trade secrets from their previous employer"; and (4) "[a]ll employees are specifically told not to speak negatively of their previous employer[.]"

45. None of First Due's representations turned out to be accurate.

46. Worse, the departing employees were solicited by First Due to steal ImageTrend's intellectual property as they were preparing to leave.

47. For example, upon information and belief, Spring was already being solicited to join First Due sometime in July 2021. Upon information and belief, on or around August 2, 2021, Spring applied to work at First Due.

48. On July 22, July 27 and August 20, 2021, Spring connected an external hard drive to his ImageTrend computer and, based on information and belief, absconded with a high volume of ImageTrend information. In particular, it is believed that Spring took ImageTrend backup data, project management files, Elite programming information/files and ImageTrend's customized SQL scripts. ImageTrend's customized SQL scripts provide a road map of the architecture of the Elite Platform and would greatly simplify the reverse engineering of the Elite Platform. The external hard drive was never returned to ImageTrend.

49. On August 12 and September 3, Spring connected his ImageTrend computer to an unidentified computer/s via a combination USB cable/software package. The primary purpose of such USB cable/software packages is to copy or synchronize data between computers. Upon information and belief, Spring used this technology to steal additional confidential and proprietary ImageTrend information. Spring never informed ImageTrend management or IT staff of his use of this technology.

50. Likewise, it is believed that Koistinen was also being solicited to join First Due in July 2021.

51. On July 12, 2021, Koistinen utilized a USB device on her ImageTrend computer. This USB device has never been returned to ImageTrend.

52. On September 1, 2021 (eight days prior to announcing her departure), Koistinen attended an internal sales meeting at ImageTrend. During and after that meeting, Koistinen sent ImageTrend's confidential and proprietary information that was being discussed *during the meeting* directly to Hulsether at First Due. The confidential and

proprietary information disclosed confidential strategic business plans and sensitive client information including meeting notes related to an ImageTrend client that was simultaneously being actively and aggressively solicited by First Due.

53. ImageTrend knows that Koistinen surreptitiously disclosed this sensitive information to Hulsether because: (1) Koistinen confessed that she provided such information to ImageTrend employees; and (2) upon receipt of the information, Hulsether immediately sent messages to an ImageTrend employee disputing the information shared in the private sales meeting.

54. On September 3, seconds after logging on to her personal Google account, Koistinen attempted to access, then altered the permissions to and did access, confidential and proprietary ImageTrend information. Shortly thereafter and repeatedly between September 3 and September 7, Koistinen accessed identically named content on her personal Google Drive. In particular, Koistinen had a file on her ImageTrend computer named "ImageTrend Implementation Schedule 7.23.21." and a file in her personal Google Drive with the same name. The ImageTrend computer version of this file contains specific and detailed information regarding a current software project being implemented by ImageTrend for its largest client. The information contained in the document includes confidential and proprietary information specifically tailored for ImageTrend's client for this particular project including the project charter, project status, obstacles, customer contact information, and specific product information and implementation. Upon information and belief, the Koistinen personal Google Drive version of this file derives

from the ImageTrend computer version of this file and Koistinen is still in possession of the Google drive version of this file.

55. Upon information and belief, Koistinen provided the information that she had taken while employed by ImageTrend to First Due.

56. In particular, upon information and belief, Koistinen provided First Due with a unique client implementation and support document containing specific and detailed information regarding a current software project being implemented by ImageTrend for its largest client. The information contained in this document included confidential and proprietary information specifically tailored for ImageTrend's client for this particular project including the project charter, project status, obstacles, customer contact information, and specific product information and implementation.

57. Upon information and belief, First Due was and is actively and aggressively soliciting this particular client identified.

58. Upon further information and belief, Koistinen, Hulsether, and First Due thereafter used this specific information pertaining to the current status and obstacles of the project to reach out to ImageTrend's client mid-project to cast doubt and aspersions on ImageTrend's implementation. The unlawfully appropriated information was used for the benefit of First Due to the detriment of ImageTrend in an effort to tortiously interfere with ImageTrend's current business relationship in order to sabotage the project and usurp the client business.

59. On September 9, 2021 (the day of her departure), Koistinen connected her ImageTrend computer to an unidentified computer/s via a combination USB cable/software

package. The primary purpose of such USB cable/software packages is to copy or synchronize data between computers. Upon information and belief, Koistinen used this technology to steal additional confidential and proprietary ImageTrend information. Koistinen never informed ImageTrend management or IT staff of her use of this technology.

60. On September 9, 2021, Koistinen, Sergio Nardi, and Spring resigned. Koistinen, an Elite Product Sales Executive, Nardi, a Client Account Advisor, and Spring, the Elite Product Manager, all informed ImageTrend that they were resigning to join First Due. Upon information and belief, Spring was hired by First Due to reverse-engineer ImageTrend's Elite product and develop for First Due a competitive EMS solution. As ImageTrend's Elite Product Manager, and in the months leading up to departing for First Due, Spring produced detailed comparative market analysis of First Due and ImageTrend solutions.

61. Upon further information and belief, Koistinen, Sergio Nardi, and Spring were recruited to join First Due by Dillard, Ritt, and Hulsether.

62. On September 13, 2021, Justin Kelly, an Account Executive, resigned to join First Due. Upon information and belief, Kelly was recruited to First Due by Hulsether and Ritt.

63. On September 14, 2021, Haley Koepke, an Implementation Lead, resigned to join First Due. Upon information and belief, Koepke was recruited by Hulsether and Koistinen.



64. On October 4, 2021, Eric Bambard, another Account Executive, resigned to join First Due. Upon information and belief, Bambard was recruited by Ritt and Hulsether.

65. On November 14, 2021, Christen Dockter, an Account Advisor and Implementation Lead, resigned to join First Due. Upon information and belief, Dockter was recruited by Hulsether.

66. On November 17, 2021, Evan Kelly, a Client Services Specialist for ImageTrend, resigned to join First Due. Upon information and belief, Kelly was recruited by Hulsether.

67. On December 14, 2021, Dutcher, an Account Advisor and Implementation Lead, resigned to join First Due. Upon information and belief, Dutcher was also recruited by Hulsether.

68. Also on December 14, 2021, Dutcher emailed ImageTrend's confidential and proprietary information to his personal email for use at First Due, including confidential client information related to one of ImageTrend's largest clients. Upon information and belief, First Due is actively and aggressively soliciting the client identified in Dutcher's email. Also upon information and belief, First Due used the confidential and proprietary information misappropriated by Hulsether, Koistinen, and Dutcher regarding ImageTrend's largest client in an attempt to interfere with and sabotage an ongoing software implementation project for this particular client. Dutcher subsequently admitted to his theft in communications with ImageTrend employees.

69. Over the past several months, First Due and the Departed Employees have continued to solicit ImageTrend's employees to leave and join them at First Due. In

connection with these solicitations, First Due and the Departed Employees have repeatedly disparaged ImageTrend. In fact, First Due's recruitment pitch—executed by the Departed Employees—is so aggressive that numerous ImageTrend employees have complained to ImageTrend senior management that they feel harassed. These solicitations continued throughout 2021.

**First Due Unlawfully Obtains Unauthorized Access to an  
ImageTrend Client Account in an Attempt to Reverse Engineer  
ImageTrend's Proprietary Software**

70. On January 5, 2022, ImageTrend executed a security scan of the ImageTrend production infrastructure. This was done, in part, through examining IP addresses — a unique string of characters that identifies each unique computer communicating over a network or the internet. ImageTrend catalogs all IP traffic on its corporate network, including employees' remote access, so ImageTrend knows the IP addresses of the devices ImageTrend's employees use/used to remotely access ImageTrend's corporate network.

71. During its investigation, ImageTrend identified that a static IP address that was accessing the Elite Platform was identical to the IP address that former ImageTrend employee Spring had previously and consistently used to remotely access the ImageTrend corporate network. More concerning, ImageTrend's investigation revealed that Spring's access of the Elite Platform occurred through an access account created by and provided only to an ImageTrend client: Staunton (Virginia) Fire Department.

72. Staunton Fire utilizes the Elite Platform to document emergency medical and fire rescue events, which include protected patient health information. Elite System

Administrators are responsible for proper Elite user account creation and management, and are expected to maintain HIPAA, data privacy, and contractual compliance.

73. French is the Staunton Fire Elite System Administrator and a First Due employee. In his role as Staunton Fire's Elite System Administrator, French had the most comprehensive, confidential, and privileged access to the Elite client application, providing French with access to ImageTrend's proprietary user interface design, database schema, dataset management tools, mapping interface and set-up, forms manager, manuals, documented deliverables, product roadmaps, templates, and protected patient health information.

74. Upon discovering the improper access, ImageTrend immediately initiated its Security Incident Response Plan. This included tendering a Notice of Security Incident to Staunton Fire and the Attorney for the City of Staunton on January 7, 2022 (attached as Exhibit A).

75. ImageTrend pulled the IP address logs for all access to the Staunton Fire Department Elite site for the previous six months. ImageTrend identified additional unknown anomalous IP addresses that had accessed the Staunton Fire Department Elite site.

76. ImageTrend discovered that the Staunton Fire Elite site had been underhandedly accessed through two usernames: the "french" account, which Defendant French uses as the System Administrator for Staunton Fire's Elite System; and a "demoadmin" username, which was created by French on October 13, 2021— one day after French began his employment with First Due.

77. ImageTrend discovered that the static IP address belonging to Spring's device was used to access the Staunton Fire Elite site using the "demoadmin" username 10 times between October 13, 2021, and January 5, 2022. In addition, it was also discovered that an IP address belonging to former employee Koistinen was also used to access the Staunton Fire Elite site 17 times between October 13, 2021, and December 29, 2021.

78. Since Koistinen and Spring's employment with ImageTrend ended on September 9, 2021, there was no legitimate basis for Koistinen or Spring to be accessing the Elite Platform, especially through a client production site. During the time period of Koistinen and Spring's unauthorized access, ImageTrend conducted nine software updates to Elite. As such, Koistinen and Spring (and others at First Due) also unlawfully gained access to the new information and innovations contained in these system updates.

79. In light of Koistinen and Spring's intimate knowledge of Elite given their previous employment with ImageTrend and the fact that they had no legitimate or lawful basis to access ImageTrend's software, the purpose of their unauthorized access was in order to reverse engineer the software and mine the new information and innovations contained in the system updates.

80. ImageTrend also discovered that a foreign IP address located in Europe accessed the Staunton Fire Elite site three times via the "demoadmin" username, all on October 13, 2021. This same foreign IP address used the "french" username to access the Staunton Fire Elite site three additional times, also all on October 13, 2021.

81. On October 14, 2021, a different foreign IP address also located in Europe used the "french" system administrator account to access the Staunton Fire Elite site.

82. Through its investigation of the electronically stored information, ImageTrend also discovered that users utilizing the “demoadmin” account had attempted to delete or obscure their audit trails and account information evidencing their access and use of the site in an attempt to hide their unlawful actions. Tellingly, on January 7, 2022, French deleted the “demoadmin” account within hours of ImageTrend tendering its Notice of Security Incident to Staunton Fire and the Attorney for the City of Staunton.

83. First Due has resources located in Europe that it utilizes for product development. Upon information and belief, the two foreign IP addresses that accessed the Staunton Fire Elite site on October 13 and 14, 2021, belong to devices used by individuals affiliated with First Due’s product-development operations in Europe.

84. Upon further information and belief, French provided the access credentials to the “demoadmin” account and the “french” account he maintained in conjunction with his employment with the Staunton Fire Department to First Due, including Spring, other First Due employees, and First Due developers overseas.

85. Upon information and belief, First Due hired French as an inducement for him to provide access to the “demoadmin” and “french” accounts.

86. Upon further information and belief, First Due’s goal in gaining access to the “demoadmin” and “french” accounts of the Staunton Fire Elite site was to attempt to reverse engineer ImageTrend’s intellectual property.

87. Through French’s position as a current ImageTrend client and Koistinen and Spring’s intimate knowledge of ImageTrend’s Elite product derived from their former employment with ImageTrend, First Due gained illegal access to and acquired confidential,

non-public, and proprietary information belonging to ImageTrend that constitutes trade secrets, including but not limited to unlawfully gaining full access to the Elite University software platform, which provides access to and displays all release notes and full documentation within the system. The Elite University software platform is not available to the general public and is only viewable by Elite clients and subject to client contracts with intellectual property and confidentiality provisions. In effect, Staunton's access level combined with Koistinen and Spring's intimate knowledge of the system would have provided First Due with the "road map" to reverse engineer or design a competitive software to the Elite Platform.

88. Furthermore, French was aware of the contract governing the Staunton Fire Department's use of ImageTrend's intellectual property. Despite having actual knowledge of that agreement, French and First Due, vis-à-vis its employment of French, caused the Staunton Fire Department to breach the agreement through French's actions.

89. These breaches of the agreement included without limitation, violation of the contract's provision against misuse of the software: "[Staunton Fire] shall not modify, reverse engineer, disassemble, or decompile the Software, or any portion thereof, and shall not use the software or portion thereof for purposes other than as intended and provided for in this Agreement."

90. Furthermore, French's actions directly violated the contract's Maintenance of Confidential Information provision: "Each party agrees to keep confidential all confidential information disclosed to it by the other in accordance herewith, and to protect

the confidentiality thereof in the same manner it protects the confidentiality of similar information and data of its own.”

91. In addition, First Due’s access of ImageTrend’s intellectual property, through French’s actions, perpetuated a violation of the Health Insurance Portability and Accountability Act (“HIPAA”) by potentially exposing protected health information to unauthorized third parties, including third parties that reside overseas.

92. Presently, First Due has not yet released a comparable competitive EMS software solution.

93. Upon information and belief, First Due is attempting to develop a competitive EMS platform, and its targeted solicitation of ImageTrend employees, inducement to encourage ImageTrend employees to steal ImageTrend’s confidential and proprietary information, and underhanded and illicit access to an ImageTrend client account to try and reverse engineer ImageTrend’s software were unlawful steps taken in furtherance of First Due’s goal to create a competitive software program for emergency medical services departments.

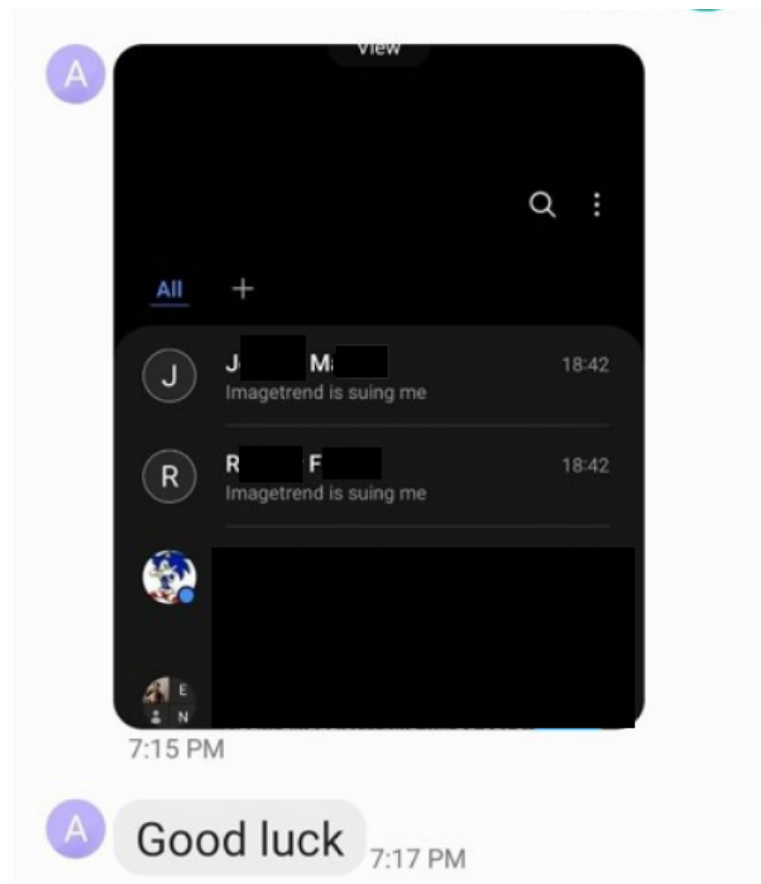
**Hulsether Defames ImageTrend to its Clients  
In Response to Receiving a Preservation Notice**

94. Upon discovering First Due’s scheme to surreptitiously access the Staunton Fire Elite site in an attempt to reverse engineer ImageTrend’s software, ImageTrend sent preservation demands to First Due and the Departed Employees on January 10, 2022.

95. That same day, Hulsether sent a threatening text message to Joe Graw, ImageTrend’s President:



96. In response, Mr. Graw questioned what Hulsether meant. Hulsether replied with a screenshot of two text messages she sent to long-standing ImageTrend clients, currently being solicited by First Due, reading “Imagetrend is suing me” and telling Mr. Graw, “Good luck”:





97. The unmistakable implication of Hulsether's text messages to the ImageTrend clients was that ImageTrend was pursuing legal action against Hulsether for illegitimate and/or improper means.

98. The implication of Hulsether's text messages is false and defamatory and tends to prejudice ImageTrend's credit and business operations as it was published to at least two of ImageTrend's clients.

**COUNT I:  
MISAPPROPRIATION OF TRADE SECRETS  
VIOLATION OF MINNESOTA'S TRADE SECRETS ACT  
(Against All Defendants)**

99. ImageTrend incorporates by reference the foregoing paragraphs as though fully set forth herein.

100. Defendants misappropriated ImageTrend's trade secrets, including without limitation, highly sensitive confidential prospective sales leads reports, current customer lists, client contact information, client support case information, client implementation plans, client contracts, custom development planning, comparative market and product analysis, confidential and proprietary information disclosed during the internal meeting on September 1, 2021, strategic business and operational plans known only to ImageTrend executive management, and certain highly-sensitive, password protected information related to ImageTrend's proprietary Elite Platform, including, but not limited to customized SQL scripts, Elite product Release Notes, Elite product roadmaps, Preset Values, Event Visibility, Form Manager, Print Report Manager, Dynamic/Situational Tools, Worksheet Manager, CQI Module and Workflows, Validation Engine, ImageTrend Library, third-

party product integration information, and Elite product training curriculum that was wrongfully obtained through the improper access of the Staunton Fire Elite site.

101. ImageTrend's trade secrets derive independent economic value from its demonstrable competitive value to other persons and entities.

102. ImageTrend's aforementioned trade secrets derive their economic benefit by not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from their disclosure or use.

103. ImageTrend intended to keep the aforementioned trade secrets confidential.

104. ImageTrend engaged in efforts that are reasonable under the circumstances to maintain the secrecy of its trade secrets. These means included without limitation, password protection of such information, continuous vulnerability scanning and external penetration testing, annual third-party security assessments, limited distribution of such information to only HIPAA trained employees, mandatory annual training on how to protect client data and company trade secrets, requiring employees to annually affirm and abide by the IP Policy and ongoing confidentiality obligations, and requiring clients (including Staunton Fire) to abide by and sign agreements designed to protect ImageTrend's confidential and proprietary information.

105. Defendants' theft and misappropriation of ImageTrend's trade secrets were gained to the benefit of Defendants and at the expense of ImageTrend.

106. ImageTrend has suffered and will continue to suffer irreparable harm through Defendants' theft and misappropriation of ImageTrend's trade secrets. As a result,

ImageTrend seeks an injunction precluding Defendants from using its trade secrets and requiring Defendants to return all trade secrets stolen pursuant to Minn. Stat. § 325C.02.

107. In addition, ImageTrend seeks compensatory damages, including the actual loss caused by misappropriation and the unjust enrichment caused by misappropriation that is not taken into account in computing actual loss, which exceed \$75,000, in an amount to be determined at trial.

108. Because Defendants' misappropriation was willful and malicious, ImageTrend also seeks exemplary damages and all attorney fees incurred in this action pursuant to Minn. Stat. § 325C.03-.04.

**COUNT II:  
MISAPPROPRIATION OF TRADE SECRETS  
VIOLATION OF DEFEND TRADE SECRET'S ACT  
(Against All Defendants)**

109. ImageTrend realleges and incorporates by reference each and every allegation stated above.

110. ImageTrend possesses confidential information and trade secrets related to its sales leads reports, current customer lists, strategic business and operational plans known only to ImageTrend management, and proprietary, password-protected information related to ImageTrend's proprietary Elite software. These trade secrets are used in and intended to be used in interstate commerce.

111. Defendants have acquired and have used or are planning to use the aforementioned trade secrets in which they knew or had reason to know that the ImageTrend trade secrets were obtained unlawfully and without authorization. For

example, the following confidential information was unlawfully misappropriated and disclosed without authorization: sales leads reports, client contact information, current customer lists, client contact information, client support case information, client implementation plans, client contracts, custom development planning, comparative market and product analysis, confidential and proprietary information disclosed during the internal meeting on September 1, 2021, strategic business and operational plans known only to ImageTrend executive management, and certain highly-sensitive, password protected information related to ImageTrend's proprietary Elite software, including, but not limited to customized SQL scripts, Elite product Release Notes, Elite product roadmaps, Preset Values, Event Visibility, Dataset Manager, Mapping Engine, Permission Objects, ImageTrend University, Form Manager, Print Report Manger, Dynamic/Situational Tools, Worksheet Manager, CQI Module and Workflows, Validation Engine, ImageTrend Library, third-party product integration information, and Elite product training curriculum that were wrongfully obtained through the improper access of the Staunton Fire Elite site.

112. The aforementioned trade secrets are related to emergency medical and fire rescue products and services used in and intended to be used in interstate commerce.

113. ImageTrend has taken reasonable steps to maintain the confidential nature of the aforementioned trade secrets, including but not limited to password protection of such information, continuous vulnerability scanning and external penetration testing, annual third-party security assessments, limited distribution of such information to only HIPAA trained employees, mandatory annual training on how to protect client data and company trade secrets, requiring employees to annually affirm and abide by the IP Policy and

ongoing confidentiality obligations, and requiring clients (including Staunton Fire) to abide by and sign agreements designed to protect ImageTrend's confidential and proprietary information.

114. The aforementioned trade secrets are nonpublic and confidential, are not generally known in the industry or elsewhere, and are not readily ascertainable through proper means by other persons.

115. The aforementioned trade secrets derive actual and potential independent economic value from not being generally known to, or readily ascertainable through proper means by, other persons who might obtain economic value from their disclosure or use, and provide ImageTrend with an economic and competitive advantage in the market.

116. Defendants possess the aforementioned trade secrets without any color of right.

117. Defendants' actions in misappropriating the aforementioned trade secrets were done willfully and maliciously.

118. Defendants' activities have involved and will continue to involve threatened and actual misappropriation, disclosure, use, or sale of ImageTrend's trade secrets, without ImageTrend's express or implied consent, and with the knowledge that this information was acquired under circumstances giving rise to a duty to maintain its secrecy and limit its use. As such, these actions constitute violations of the Defend Trade Secrets Act of 2016 and 18 U.S.C. § 1836.

119. Defendants' misappropriation of the aforementioned trade secrets has caused and will continue to cause direct, irreparable harm and actual damages to ImageTrend

including, but not limited to, injury to its business and business relationships in excess of \$75,000, in an amount to be determined at trial, as well as injunctive relief, exemplary damages, and attorneys' fees.

**COUNT III:  
BREACH OF FIDUCIARY DUTY  
(Against Dutcher, Hulsether, and Koistinen)**

120. ImageTrend incorporates by reference the foregoing paragraphs as though fully set forth herein.

121. As employees of ImageTrend, the Dutcher, Hulsether, and Koistinen owed ImageTrend fiduciary duties, including the duties of care and loyalty.

122. Dutcher, Hulsether, and Koistinen breached their fiduciary duties to ImageTrend. Their breaches include, without limitation: (1) soliciting multiple agents to terminate their relationships with ImageTrend prior to ending their employment with ImageTrend; (2) actively competing with ImageTrend prior to ending their employment with ImageTrend and, in the case of Hulsether, being employed by First Due before ending her employment with ImageTrend; (3) taking proprietary and confidential information from ImageTrend to First Due before leaving ImageTrend's employ; and (4) deleting many electronic files related to their work.

123. As a direct and proximate result of Dutcher, Hulsether, and Koistinen's breaches of their fiduciary duties, ImageTrend seeks compensatory damages in excess of \$75,000, in an exact amount to be determined at trial. ImageTrend also seeks disgorgement of amounts paid to Dutcher, Hulsether, and Koistinen by First Due as ill-gotten gains.

**COUNT IV:  
UNJUST ENRICHMENT, CONSTRUCTIVE TRUST, AND ACCOUNTING  
(Against First Due)**

124. ImageTrend incorporates by reference the foregoing paragraphs as though fully set forth herein.

125. To the extent that any of the allegations pertaining to misappropriation of confidential and proprietary information do not constitute “trade secrets” as defined under the Defend Trade Secrets Act of 2016, Count IV and the following allegations are pled in the alternative:

126. To the extent that First Due has obtained any income or financial benefit as a result of breaches of contract, breaches of fiduciary duties, and unfair competition as set forth above, it has unjustly enriched itself at ImageTrend’s expense.

127. As a direct and proximate result of this unfair competition, ImageTrend is entitled to the imposition of a constructive trust and an accounting for recovery of all income and financial benefits that First Due has obtained and received as a result of its wrongful misconduct and unfair competition.

**COUNT V:  
CIVIL CONSPIRACY  
(Against All Defendants)**

128. ImageTrend restates and realleges the foregoing Paragraphs as though fully set forth herein.

129. To the extent that any of the allegations pertaining to misappropriation of confidential and proprietary information do not constitute “trade secrets” as defined under

the Defend Trade Secrets Act of 2016, Count V and the following allegations are pled in the alternative:

130. Defendants initiated a campaign to utilize unlawful and malicious tactics to poach ImageTrend employees by disparaging ImageTrend and harassing its employees. In addition, Defendants' campaign further included coercion and solicitation of ImageTrend employees to conspire with First Due to intentionally and unlawfully misappropriate and steal ImageTrend's trade secret information.

131. The purpose of Defendants' campaign to poach ImageTrend employees was to misappropriate and steal ImageTrend's trade secret information, which constitutes unlawful conduct and was perpetrated through unlawful means without ImageTrend's authorization or consent.

132. As a result, Defendants are jointly and severally liable for all damages caused by their conduct.

133. As a direct and proximate result of Defendants' civil conspiracy, ImageTrend has been damaged in excess of \$75,000, in an amount to be determined at trial. ImageTrend is also entitled to injunctive relief to prevent continued and future misappropriation of ImageTrend's trade secrets.

**COUNT VI:  
CIVIL THEFT  
(Against All Defendants)**

134. ImageTrend restates and realleges the foregoing Paragraphs as though fully set forth herein.



135. To the extent that any of the allegations pertaining to misappropriation of confidential and proprietary information do not constitute “trade secrets” as defined under the Defend Trade Secrets Act of 2016, Count VI and the following allegations are pled in the alternative:

136. The trade secret information described herein constitutes personal property under Minn. Stat. § 604.14.

137. Defendants intentionally took and continue to possess ImageTrend’s trade secret information without claim of right and with intent to deprive ImageTrend of the value of its possession.

138. Defendants’ possession of the trade secret information amounts to civil theft as defined by Minn. Stat. § 604.14 and § 609.52.

139. As a result of Defendants’ theft, ImageTrend is entitled to damages against them in excess of \$75,000, and as defined by § 604.14, subd. 1, including the value of the trade secret information when stolen plus 100% of that value.

**COUNT VII:  
TORTIOUS INTERFERENCE WITH CONTRACT  
(Against First Due regarding Staunton Fire)**

140. ImageTrend restates and realleges the foregoing Paragraphs as though fully set forth herein.

141. First Due was aware of the agreement between ImageTrend and its customer, Staunton Fire, and the terms and conditions therein. First Due intentionally and improperly procured and encouraged the continuing breaches of the terms and conditions set forth in the agreement, including but not limited to encouraging its employees French and Spring

to set up an account, utilize, and misappropriate ImageTrend's trade secrets, proprietary, and confidential information.

142. As a direct and proximate cause of First Due's efforts to tortiously interfere with the agreement, ImageTrend has been damaged in an amount in excess of \$75,000, in an exact amount to be proven at trial.

143. To the extent the allegations of this Count include misappropriation of trade secrets as defined under the Defend Trade Secrets Act of 2016, ImageTrend seeks recovery beyond such misappropriation, including as it concerns the method and manner defendants used to accomplish the alleged misappropriations, the illicit tactics used to derive competitive advantage because of the illegitimate and unauthorized access, and the ImageTrend resources required to address the breach.

144. To the extent that any of the allegations pertaining to misappropriation of confidential and proprietary information do not constitute "trade secrets" as defined under the Defend Trade Secrets Act of 2016, Count VII is pled in the alternative.

145. ImageTrend is also entitled to an injunction, and its reasonable attorneys' fees and costs against First Due for having to prosecute its tortious interference with contract claims against First Due.

**COUNT VIII**  
**TORTIOUS INTERFERENCE WITH CONTRACTUAL RELATIONS,**  
**PROSPECTIVE CONTRACTUAL RELATIONS,**  
**AND/OR PROSPECTIVE ECONOMIC RELATIONS**  
**(Against First Due)**

146. ImageTrend realleges and incorporates by reference each and every allegation stated above.

147. ImageTrend maintains contractual, prospective contractual and prospective economic relations with current and potential clients. ImageTrend further maintains contractual and economic relations with its current employees.

148. ImageTrend has a reasonable expectation of prospective contractual, and/or economic relations with current and potential clients. ImageTrend further has a reasonable expectation of contractual and economic relations with its current employees.

149. First Due knew of ImageTrend's relations and reasonable expectations of relations with current and potential clients. For instance, First Due knew of the current contractual and economic relationship with its largest customer. First Due knew that ImageTrend was in the process of a significant implementation project for its largest client. First Due knew of ImageTrend's relations and reasonable expectation of relations with its current employees.

150. First Due wrongfully interfered with ImageTrend's relations and reasonable expectation of relations with current and potential clients, without justification. For instance, First Due induced current and former ImageTrend employees to misappropriate confidential and proprietary information regarding the implementation project for ImageTrend's largest client and provide that information to First Due. First Due used the

confidential and proprietary information misappropriated by Hulsether, Koistinen, and Dutcher regarding ImageTrend's largest client in an attempt to interfere with and sabotage an ongoing software implementation project for its largest client in order to tortiously interfere with ImageTrend's contractual relationship with its client.

151. First Due further wrongfully interfered with ImageTrend's relations and reasonable expectations of relations with its current employees without justification in that it solicited and coerced ImageTrend employees to wrongfully misappropriate and steal trade secret information.

152. In the absence of First Due's wrongful interference, it is reasonably probable that ImageTrend would have realized its reasonable expectations. Further, in the absence of First Due's wrongful interference with its employee relationships, ImageTrend's trade secret information would not have been misappropriated and it would have realized further economic relations.

153. First Due's tortious interference with ImageTrend's relations and reasonable expectations of relations has caused, and continues to cause, ImageTrend legal and equitable harm.

**COUNT IX**  
**CORPORATE DEFAMATION**  
**(Against First Due and Hulsether)**

154. ImageTrend realleges and incorporates by reference each and every allegation stated above.

155. Hulsether published the following statement via text message to two ImageTrend clients on January 10, 2022: "Imagetrend is suing me."

156. The unmistakable implication of Hulsether's text messages to the ImageTrend clients was that ImageTrend was pursuing legal action against Hulsether for illegitimate and/or improper means.

157. The implication of Hulsether's text messages is false and defamatory.

158. Hulsether's text messages tend to prejudice ImageTrend's credit and business operations as it was published to at least two of ImageTrend's clients.

159. First Due is vicariously liable for Hulsether's statements.

160. ImageTrend is entitled to presumed damages as a result of Hulsether's statements.

### **JURY TRIAL DEMANDED**

1. Plaintiff demands a jury trial on all issues so triable.

### **PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiff requests that the Court enter judgment against Defendant as follows:

1. Enjoining First Due from using ImageTrend's confidential information and requiring First Due to return to ImageTrend all confidential information it stole;

2. Enjoining First Due from soliciting employees of ImageTrend during the pendency of this action;

3. Enjoining First Due from soliciting customers and potential customers of ImageTrend during the pendency of this action;

4. Enjoining First Due from using or misappropriating ImageTrend's trade secrets and requiring First Due to return all trade secrets it stole pursuant to Minn. Stat. § 325C.02;

5. Imposing a constructive trust and ordering that First Due is liable to account for and pay over to ImageTrend any and all income or other financial benefit or profit it has received as a result of its misconduct and unfair competition;

6. Awarding ImageTrend compensatory damages in an amount to be proven at trial but reasonably believed to be in excess of \$75,000.00;

7. Awarding ImageTrend exemplary damages and all attorney fees incurred in this action pursuant to Minn. Stat. § 325C.03-.04;

8. An award of Plaintiffs' costs, disbursements, prejudgment interest and expert witness fees incurred herein; and

9. An award of such other further relief as the Court finds appropriate.

**BASSFORD REMELE**  
***A Professional Association***

Date: April 8, 2022

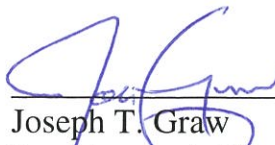
/s/Jessica L. Klander  
Jessica L. Klander (#392290)  
Jeffrey R. Mulder (#389205)  
Daniel R. Olson (#389235)  
100 South 5th Street, Suite 1500  
Minneapolis, MN 55402-1254  
Telephone: (612) 333-3000  
Facsimile: (612) 333-8829  
jklander@bassford.com  
jmulder@bassford.com  
dolson@bassford.com

*Attorneys for Plaintiff ImageTrend, Inc.*

**VERIFICATION**

Joseph T. Graw hereby states and declares that he is the President and Chief Operating Officer; that he is duly authorized to execute this Verification of behalf of the Plaintiff in the above-captioned action; that he has read the foregoing Verified Complaint and knows the contents thereof; and that the same is true to the best of his knowledge, except for those matters therein alleged upon information and belief, and as to those matters, he believes them to be true.

Dated: 4/8/2022

  
\_\_\_\_\_  
Joseph T. Graw  
President and Chief Operating Officer  
ImageTrend, Inc.